(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. Februar 2001 (22.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/13230 A1

(51) Internationale Patentklassifikation[7]: G06F 11/00

(21) Internationales Aktenzeichen: PCT/AT00/00174

(22) Internationales Anmeldedatum:
26. Juni 2000 (26.06.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 1395/99 13. August 1999 (13.08.1999) AT

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **FTS COMPUTERTECHNIK GES.M.B.H.** [AT/AT]; Föhrenweg 8, A-2500 Baden-Siegenfeld (AT).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KOPETZ, Hermann** [AT/AT]; Föhrenweg 8, A-2500 Baden-Siegenfeld (AT). **KOPETZ, Georg** [AT/AT]; Föhrenweg 8, A-2500 Baden-Siegenfeld (AT).

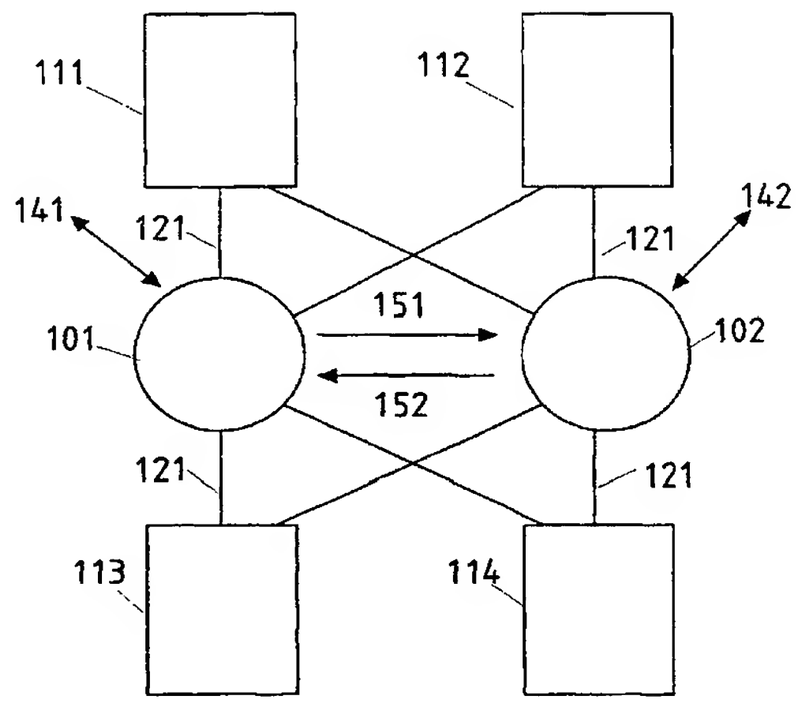
(74) Anwalt: **MATSCHNIG, Franz**; Siebensterngasse 54, A-1070 Wien (AT).

(81) Bestimmungsstaaten *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR IMPOSING THE FAIL-SILENT CHARACTERISTIC IN A DISTRIBUTED COMPUTER SYSTEM AND DISTRIBUTION UNIT IN SUCH A SYSTEM

(54) Bezeichnung: VERFAHREN ZUM ERZWINGEN DER FAIL-SILENT EIGENSCHAFT IN EINEM VERTEILTEN COMPUTERSYSTEM UND VERTEILEREINHEIT EINES SOLCHEN SYSTEMS



(57) Abstract: The invention relates to a method for imposing the fail-silent characteristic in the time period of servers (111...114) pertaining to a fault-tolerant distributed computer system wherein a plurality of servers are connected via a distribution unit (101, 102). Each server is provided with an autonomous communication control unit with the corresponding connections to the communication channels (121). Access to the communication channels is given according a cyclical time slice method. The at least one distribution unit which a priori knows the regular transmission behaviour of the servers imposes that a server is only capable to transmit to the remaining servers within the statically allocated time slice thereof.

(57) Zusammenfassung: Verfahren zum Erzwingen der fail-silent Eigenschaft im Zeitbereich von Knotenrechnern (111...114) eines fehlertoleranten verteilten Computersystems, in dem eine Vielzahl von Knotenrechnern über eine Verteilereinheit (101, 102) verbunden sind, jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit mit den entsprechenden Anschlüssen an die Kommunikationskanäle (121) verfügt und der Zugriff auf die Kommunikationskanäle entsprechend einem zyklischen Zeitscheibenverfahren erfolgt. Dabei erzwingt die zumindest eine Verteilereinheit aufgrund des ihr a priori bekannten regulären Sendeverhaltens der Knotenrechner, dass ein Knotenrechner nur innerhalb seiner statisch zugewiesenen Zeitscheibe an die anderen Knotenrechner zu senden vermag.

WO 01/13230 A1

EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *Mit internationalem Recherchenbericht.*

— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

VERFAHREN ZUM ERZWINGEN DER FAIL-SILENT EIGENSCHAFT IN EINEM VERTEILTEN COMPUTERSYSTEM UND VERTEILEREINHEIT EINES SOLCHEN SYSTEMS

Diese Erfindung betrifft ein Verfahren zum Erzwingen der fail-silent Eigenschaft im Zeitbereich von Knotenrechnern eines fehlertoleranten verteilten Computersystems, in dem eine Vielzahl von Knotenrechnern über eine Verteilereinheit verbunden sind, jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit mit den entsprechenden Anschlüssen an die Kommunikationskanäle verfügt und der Zugriff auf die Kommunikationskanäle entsprechend einem zyklischen Zeitscheibenverfahren erfolgt. Ebenso betrifft die Erfindung eine Verteilereinheit mit integriertem Guardian zur Erzwingung der fail-silent Eigenschaft im Zeitbereich von Knotenrechnern eines fehlertoleranten verteilten Computersystems, über welche eine Vielzahl von Knotenrechnern miteinander verbunden sind, jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit mit zugehörigen Anschlüssen an die Kommunikationskanäle verfügt und der Zugriff auf die Kommunikationskanäle entsprechend einem zyklischen Zeitscheibenverfahren erfolgt.

Sicherheitskritische technische Anwendungen, d.s. insbesondere Anwendungen, bei welchen ein Fehler zu einer Katastrophe führen kann, werden zunehmend von verteilten fehlertoleranten Echtzeitcomputersystemen geführt.

In einem verteilten fehlertoleranten Echtzeitcomputersystem, bestehend aus einer Anzahl von Knotenrechnern und einem Echtzeitkommunikationssystem, muss der Ausfall eines Knotenrechners toleriert werden. Im Kern einer solchen Computerarchitektur befindet sich ein fehlertolerantes Echtzeitkommunikationssystem zum vorhersehbar schnellen und sicheren Austausch von Nachrichten.

Ein Kommunikationsprotokoll, das diese Anforderungen erfüllt, ist in der EP 0 658 257 A (WO 94/06080) beschrieben. Dieses Protokoll ist unter dem Namen „Time-Triggered Protokoll/C (TTP/C)“ bekannt geworden. Es basiert auf dem bekannten zyklischen Zeitscheibenverfahren (TDMA-time-division multiple access) mit a priori festgelegten Zeitscheiben. Das Protokoll TTP/C verwendet ein Verfahren zur fehlertoleranten Uhrensynchronisation, das in der US 4,866,606 A geoffenbart ist.

Das Protokoll TTP/C setzt voraus, dass das Kommunikationssystem eine logische Broadcasttopologie unterstützt und dass die Knotenrechner ein „fail-silence“ (Kopetz, p. 121) Ausfallverhalten zeigen, d.h. entweder die Knotenrechner funktionieren korrekt im Wertebereich und im Zeitbereich oder sie sind ruhig Dies ist beschrieben in Kopetz, H. (1997), „Real-Time Systems, Design Principles for Distributed Embedded Applications“; ISBN: 0-7923-9894-7, Boston, Kluwer Academic Publishers. Die Verhinderung von Fehlern im Zeitbereich, d. s. der sogenannten „Babbling Idiot“ Fehler (Kopetz, p. 130), wird in dem Protokoll TTP/C durch eine unabhängige Fehlererkennungseinheit, den sogenannten „Guardian“, erreicht, der über eine unabhängige Zeitbasis verfügt und das Zeitverhalten des Knotenrechners kontinuierlich überprüft. Um die Fehlertoleranz zu realisieren, werden mehrere fail-silent Knotenrechner zu einer fehlertoleranten Einheit (fault-tolerant unit-FTU) zusammengefasst und das Kommunikationssystem repliziert. Solange ein Knotenrechner einer FTU und ein Replikat des Kommunikationssystems funktionieren, werden die Dienste der FTU im Zeit- und Wertebereich rechtzeitig erbracht.

Eine logische Broadcasttopologie der Kommunikation kann physikalisch entweder durch ein verteiltes Bussystem, ein verteiltes Ringsystem, oder durch eine Verteilereinheit, z.B. einen Sternkoppler, mit Punkt-zu-Punkt Verbindungen zu den Knotenrechnern oder durch eine Kombination dieser Topologien aufgebaut werden. Wenn ein verteiltes Bussystem oder ein verteiltes Ringsystem aufgebaut wird, so muss jeder Knotenrechner über seinen eigenen Guardian verfügen. Wird hingegen eine Verteilereinheit verwendet, so können alle Guardians in diese Verteilereinheit integriert werden, die aufgrund der globalen Beobachtung des Verhaltens aller Knotenrechner ein reguläres Sendeverhalten im Zeitbereich effektiv erzwingen kann. Die vorliegende Erfindung betrifft auch die Integration der Guardians in eine solche Verteilereinheit.

Solche Verteilereinheiten mit integriertem Guardian bringen folgende Vorteile:

(i) Die Fault-Containment Region für global kritische Fehler wird um die Punkt-zu-Punkt Verbindungen der Knotenrechner zu der Verteilereinheit reduziert, d. h. Fehler, die z. B. durch EMI (electromagnetic immission) in diese Punkt-zu-Punkt Verbindungen eingestreut werden, können eindeutig einem Knotenrechner zugeordnet werden und haben keine globale Wirkung.

(ii) Die replizierten global kritischen Verteilereinheiten können räumlich getrennt in geschützten Bereichen installiert und physisch kompakt ausgeführt werden. Dadurch wird die Wahrscheinlichkeit, dass eine Fehlerursache alle global kritischen Verteilereinheiten zerstört, signifikant herabgesetzt.

(iii) Der Guardian der Verteilereinheit ersetzt die dezentralen Guardians in den Knotenrechnern. Dadurch wird bei den Knotenrechnern Hardware, z.B. die Guardian Oszillatoren eingespart.

(iv) Physikalische Punkt-zu-Punkt Verbindungen eignen sich gut für die Einführung von Glasfaser und bringen auch bei verdrillten Leitungen Vorteile in der Impedanzanpassung.

Es ist eine Aufgabe der Erfindung die Fehlertoleranz eines verteilten zeitgesteuerten Computersystems zu erhöhen und die Kosten zu senken.

Diese Aufgabe wird mit einem Verfahren der eingangs genannten Art gelöst, bei welchem erfindungsgemäß die zumindest eine Verteilereinheit aufgrund des ihr a priori bekannt regulären Sendeverhaltens der Knotenrechner erzwingt, dass ein Knotenrechner nur innerhalb seiner statisch zugewiesenen Zeitscheibe an die anderen Knotenrechner zu senden vermag.

Durch die Integration eines „Guardian“ in die intelligente Verteilereinheit können „Babbling Idiot“-Fehler, d.h. Aussendung von Nachrichten zu falschen Zeitpunkten, der Knotenrechner verhindert werden.

Ebenso wird die Aufgabe mit einer Verteilereinheit der oben erwähnten Art gelöst, bei welcher erfindungsgemäß die zumindest eine Verteilereinheit dazu eingerichtet ist, aufgrund des ihr a priori bekannten regulären Sendeverhaltens der Knotenrechner zu erzwingen, dass ein Knotenrechner nur innerhalb seiner statisch zugewiesenen Zeitscheibe an die anderen Knotenrechner zu senden vermag.

Die Funktion der Verteilereinheit basiert auf der Auswertung einer Kombination von statischen a priori Informationen über die zeitliche Sendeberechtigung der einzelnen Knotenrechner mit einer dynamischen Synchronisation der Verteilereinheit durch die Nachrichten eines zeitgesteuerten Kommunikationssystems.

Die Erfindung samt ihrer weiteren Vorteile wird im folgenden an Hand von Ausführungsbeispielen näher erläutert, die in der Zeichnung veranschaulicht wird. In dieser zeigen:

- Fig. 1 die Struktur eines verteilten Computersystems mit vier Knotenrechnern, die über zwei replizierte Verteilereinheiten verbunden sind,
- Fig. 2 die Struktur eines Knotenrechners, bestehend aus einer Kommunikations-Kontrolleinheit und einem Hostcomputer, die über ein Communication Network Interface (CNI) kommunizieren,

- Fig. 3 die Struktur einer Verteilereinheit mit integriertem Guardian,
- Fig. 4 die Datenstruktur der Information, welche die Verteilereinheit a priori enthält,
- Fig. 5 die Struktur einer Initialisierungsnachricht, und
- Fig. 6 die inneren Zustände der Verteilereinheit.

Im folgenden Abschnitt wird eine Realisierung der Erfindung an einem Beispiel mit vier Knotenrechnern, die über zwei replizierte Verteilereinheiten verbunden sind, gezeigt. Die Objekte in den Abbildungen sind so nummeriert, dass sich die erste der dreistelligen Bezugsziffern immer auf die Bildnummer bezieht.

Fig. 1 zeigt ein System von vier Knotenrechnern **111**, **112**, **113** und **114**, wobei jeder Knotenrechner eine austauschbare Einheit bildet und über je eine Punkt-zu-Punkt Verbindung **121** mit zwei replizierten Verteilereinheiten **101** und **102** verbunden ist. Von der ersten Verteilereinheit **101** führt ein unidirektionaler Kommunikationskanal **151** zu der anderen zweiten Verteilereinheit **102**. Umgekehrt führt von der Verteilereinheit **102** ein unidirektionaler Kommunikationskanal **152** zu der Verteilereinheit **101**. Über diese unidirektionalen Kommunikationskanäle kann die erste Verteilereinheit **101** den Verkehr auf der zweiten Verteilereinheit **102** und umgekehrt beobachten und den Kaltstart oder die Uhrensynchronisation auch vornehmen, wenn es an den eigenen Verbindungen **121** keinen Nachrichtenverkehr gibt. Angedeutete Verbindungen **141** und **142** sind dedizierte Kommunikationskanäle; sie führen zu einem auf der Zeichnung nicht ersichtlichen Wartungscomputer, der die Parameter der Verteilereinheiten festlegen kann und die korrekte Funktion der Verteilereinheiten kontinuierlich überwacht.

Fig. 2 zeigt den inneren Aufbau eines Knotenrechners **111**. Er besteht aus zwei Subsystemen, nämlich einem Kommunikationskontroller **210**, der mit den replizierten Kommunikationskanälen **201** und **202** verbunden ist (entspricht **121** in Fig. 1), und einem Hostcomputer **220**, auf dem die Anwendungsprogramme des Knotenrechners ausgeführt werden. Diese beiden Subsysteme sind miteinander über ein Communication Network Interface (CNI) **241** und eine Signalleitung **242** verbunden. Das Interface 241 enthält einen Speicher (Dual Ported RAM = DPRAM), auf den beide Subsysteme zugreifen können. Die beiden Subsysteme tauschen über diesen gemeinsamen Speicher bzw. Interface **241** die Kommunikationsdaten aus. Die Signalleitung **242** dient zur Übertragung der synchronisierten Zeitsignale. Diese Signalleitung ist in der angeführten US 4,866,606 A genau beschrieben. Der Kommunikationskontroller **210,** der autonom arbeitet, verfügt über eine Kommunikationskontrolleinheit **211** und eine Datenstruktur **212,** die angibt, zu welchen Zeitpunkten Nachrichten gesendet und empfangen werden müssen. Die Datenstruktur **212** wird als Message Descriptor List (MEDL) bezeichnet.

Fig. 3 zeigt die Struktur einer Verteilereinheit mit integriertem Guardian. Eine solche Verteilereinheit besteht aus Eingangsports **311**, Ausgangsports **312**, einem Datenverteiler **330** und einem Steuercomputer **340**. Die Datenverbindungen **309** von dem Knotenrechner (entspricht **121** in Fig. 1), werden zu einem Eingangsport **311** und einem Ausgangsport **312** der Verteilereinheit geführt. Das gleiche gilt für Datenverbindungen **302, 303** und **304**. Bei einer unidirektionalen Kommunikationsleitung können diese beiden Ports **311** und **312** auch getrennt mit entsprechenden Ports des Knotenrechners mit der Datenverbindung **301** verbunden werden. In jedem Eingangsport **311** befindet sich - neben den üblichen Filtern und, falls erforderlich, einer Potenzialtrennung - ein Schalter **313,** der vom Steuercomputer **340** der Verteilereinheit über eine Signalleitung **314** angesteuert werden kann und der dem Steuercomputer **340** mitteilt, wann auf diesem Port empfangen wird. Die Daten, die am Eingangsport **311** eintreffen, werden über den Datenverteiler **330** an die Ausgangsports **312,** an den Steuercomputer **340** (über die Datenleitung **331**) und an andere Verteilereinheiten (über den Kanal **351**) weitergeleitet. Der Steuercomputer **340** verfügt auch über einen seriellen I/O Kanal **341**, über den die statische Datenstruktur entsprechend Fig. 4 geladen werden kann und der periodisch Diagnosemeldung über den Zustand des Steuercomputers **340** an einen Wartungscomputer gibt. Falls erforderlich, können die Daten auf den Leitungen **312** vor dem Ausgang verstärkt werden. Solche, dem Stand der Technik entsprechenden Verstärker sind in der Fig. 3 nicht eingetragen.

Fig. 4 zeigt die Datenstruktur, die dem Steuercomputer **340** a priori, d.h. vor der Laufzeit, zur Verfügung gestellt wird. Diese Datenstruktur enthält für jeden Port bzw. Knotenrechner **111, 112, 113, 114** der Verteilereinheit einen eigenen Datensatz **411, 412, 413, 414**. In einem ersten Feld dieses Datensatzes **401** steht die Portnummer, auf die sich dieser Datensatz bezieht. In einem zweiten Feld **402** steht die Sendedauer des mit dem Port verbundenen Knotens entsprechend der Eintragung in der Liste MEDL **212**. In einem dritten Feld **403** steht die Dauer des Zeitintervalls zwischen dem Ende des aktuellen Sendens bis zum Beginn des nächsten Sendens des mit dem Port verbundenen Knotens. In einem vierten Feld **404** steht die Nummer des zeitlich nächsten Ports. In einem fünften Feld **405** steht die Dauer des Zeitintervalls zwischen dem Ende des aktuellen Sendens bis zum Beginn des Sendens des Knotens am zeitlich nächsten Port. Im Feld **406** steht die Länge einer Initialisierungsnachricht, die auf dem aktuellen Port empfangen werden kann. Der Inhalt der Datenstruktur von Fig. 4 wird von einem Entwicklungstool in Abstimmung mit den Message Descriptor Lists **212** erstellt und vor der Laufzeit über den Kanal **341** in den Steuercomputer **340** geladen.

Fig. 5 zeigt die Struktur einer Initialisierungsnachricht. Die Initialisierungsnachricht muss in Header **501** ein ausgezeichnetes Bit **510** enthalten, das die Nachricht als Initialisierungsnachricht kennzeichnet. Im Datenfeld **502** der Initialisierungsnachricht stehen weitere Informationen, die

für die Funktion einer einfachen Verteilereinheit ohne Bedeutung sind. Am Ende der Initialisierungsnachricht befindet sich das CRC Feld **503**. Entsprechend leistungsfähige Verteilereinheiten können die Informationen im Datenfeld **502** einer Initialisierungsnachricht zusätzlich zur Erhöhung der Fehlererkennungswahrscheinlichkeit auswerten. Zum Beispiel können solche leistungsfähigere Verteilereinheiten das Zeitfeld einer TTP/C Initialisierungsnachricht auswerten, um den Uhrenstand des Senders mit der eigenen Uhr vergleichen zu können.

Fig. 6 zeigt die beiden wichtigsten inneren Zustände des Steuercomputers **340,** einer Verteilereinheit **101**, unsynchronisiert **601** und synchronisiert **602**. Nach Power-up **610** geht der Steuercomputer **340** in den Zustand „unsynchronisiert". In diesem Zustand sind alle Eingangports **311** mit dem Datenverteiler **330** verbunden. Sobald auf einem Eingangsport über die Datenleitung **331** (oder über den Kanal **352**) vom Steuercomputer **340** eine korrekte Nachricht empfangen wird, stellt der Steuercomputer **340** über die Signalleitung **314** fest, über welchen Port empfangen wurde, speichert den Empfangszeitpunkt, überprüft die Länge der Nachricht durch Vergleich mit der im Feld **406** gespeicherten Länge und geht, bei positivem Ausgang der Prüfung, in den Zustand „synchronisiert" **602**, wobei der gespeicherte Empfangszeitpunkt der Initialisierungsnachricht das Synchronisationsereignis darstellt. Im Zustand „synchronisiert" **602** stellt der Steuercomputer **340** nur während der Zeitdauer **403** eine Verbindung am entsprechenden Eingangsport her. Wenn zum ungefähr richtigen Zeitpunkt eine beliebige Nachricht eintrifft, die den Codierungsvorschriften des gewählten Codierungssystems entspricht, dann verwendet der Steuercomputer die gemessene Zeitdifferenz zwischen dem beobachteten und erwarteten Ankunftszeitpunkt der Nachricht, um seine Uhr über einen bekannten fehlertoleranten Algorithmus (z.B. Kopetz 1997, p. 61) nachzusynchronisieren. Wenn während eines a priori festgelegten Zeitintervalls $d_{fault-1}$ keine korrekte Nachricht an irgendeinem der Kanäle **301** bis **304** oder **352** eintrifft, wechselt die Verteilereinheit bzw. ihr Steuercomputer **340** in den Zustand „unsynchronisiert" **601**. Im synchronisierten Zustand **602** ist eine Nachricht korrekt, wenn sie mindestens die folgenden Kriterien erfüllt: Sie trifft am Eingangsport ungefähr zum erwarteten Zeitpunkt ein, verfügt über ein korrektes CRC Feld **503** und hat die richtige Länge entsprechend dem Feld **406**.

Der Steuercomputer **340** kommuniziert über die I/O Leitung **341** (dies sind die Leitungen **141** und **142** in Fig. 1) mit einem Wartungscomputer, der die Parametrisierung des Steuercomputers **340** vornimmt und die Funktion des Steuercomputers während des Betriebes überwacht.

Um zu verhindern, dass ein Einzelfehler im Taktgeber eines Knotenrechners, z.B. **111**, der zu einer marginal falschen Kodierung der physikalischen Signale auf beiden Kanälen **201** und **202** des Knotenrechners **111** führen kann, über beide Verteilereinheiten an die Empfänger der Nachricht durchschlägt, wird das eintreffende physikalische Signal in jeder Verteilereinheit unmittel-

bar nach dem Empfangen unter Verwendung des lokalen Taktgebers der Verteilereinheit in ein Digitalsignal umgewandelt und unmittelbar vor dem Senden von der Verteilereinheit erneut in die physikalische Form umgewandelt (Signal Reshaping durch die Verteilereinheit). Damit wird ein marginal falsche Kodierung entweder in eine konsistent richtige Kodierung oder in eine konsistent falsche Kodierung abgebildet. Unter der Annahme, dass innerhalb einer TDMA Runde nur eine Fehlerursache auftritt, kann durch diese Maßnahme verhindert werden, dass ein Einzelfehler im Zeitbereich oder im Wertebereich die Kodierung auf beiden Kanälen derart stört, dass im System Inkonsistenzen auftreten können.

Es ist eine wichtige Eigenschaft dieser Erfindung, dass der Steuercomputer **340** nur das Öffnen und Schließen der Schalter **313** bewirken kann, jedoch die vermittelten Nachrichten inhaltlich weder verändert, noch neue Nachrichten einfügt. Die einzige Ausfallart der Verteilereinheit ist daher ein fail-silent Ausfall eines Kommunikationskanals. In einer fehlertoleranten Konfiguration ist aber stets ein zweiter unabhängiger Kommunikationskanal vorhanden.

Abschließend sei festgehalten, dass sich die Erfindung nicht auf die beschriebene Realisierung mit vier Knotenrechnern und zwei Verteilereinheiten beschränkt, sondern beliebig erweiterbar ist. Sie ist nicht nur beim TTP/C Protokoll, sondern auch bei anderen zeitgesteuerten Protokollen anwendbar.

PATENTANSPRÜCHE

1. Verfahren zum Erzwingen der fail-silent Eigenschaft im Zeitbereich von Knotenrechnern eines fehlertoleranten verteilten Computersystems, in dem eine Vielzahl von Knotenrechnern über eine Verteilereinheit verbunden sind, jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit mit den entsprechenden Anschlüssen an die Kommunikationskanäle verfügt und der Zugriff auf die Kommunikationskanäle entsprechend einem zyklischen Zeitscheibenverfahren erfolgt

   dadurch gekennzeichnet, dass

   die zumindest eine Verteilereinheit aufgrund des ihr a priori bekannten regulären Sendeverhaltens der Knotenrechner erzwingt, dass ein Knotenrechner nur innerhalb seiner statisch zugewiesenen Zeitscheibe an die anderen Knotenrechner zu senden vermag.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die zumindest eine Verteilereinheit von dem Zustand „unsynchronisiert", in dem über alle Eingangsports empfangen werden kann, nach dem Empfang einer korrekten Nachricht in den Zustand „synchronisiert" wechselt, in dem über einen Eingangsport nur während der diesem Eingangsport statisch zugewiesenen Zeitscheibe empfangen werden kann.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** die zumindest eine Verteilereinheit vom Zustand „synchronisiert" in den Zustand „unsynchronisiert" wechselt, wenn seit der letzten Initialisierungsnachricht an keinem ihrer Eingangports innerhalb eines a priori vorgegebenen Zeitintervalls eine korrekte Nachricht empfangen wird.

4. Verfahren nach einem oder mehreren der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** einer Verteilereinheit der Inhalt von eintreffenden Nachrichten im Sinne einer zusätzlichen Fehlererkennung ausgewertet wird.

5. Verfahren nach einem oder mehreren der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** die zumindest eine Verteilereinheit nach „Power-up" den Zustand „unsynchronisiert" einnimmt.

6. Verfahren nach einem oder mehreren der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** die zumindest eine Verteilereinheit die ankommenden physikalischen Signale unter Verwendung der lokalen Uhr der Verteilereinheit in die Digitalform umwandelt und vor dem Senden wieder in die physikalische Form überführt.

7. Verfahren nach einem oder mehreren der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** Verteilereinheiten über Kommunikationskanäle miteinander verbunden sind, um das Hochfahren und die Uhrensynchronisation einer Verteilereinheit zu ermöglichen, auch wenn auf den eigenen Verbindungen keine Nachrichten eintreffen.

8. Verfahren nach einem oder mehreren der Ansprüche 1 bis 6 **dadurch gekennzeichnet, dass** Verteilereinheiten über dedizierte Kommunikationskanäle mit mindestens einem Wartungscomputer verbunden sind, die die Parametrisierung der Verteilereinheiten vornehmen und die korrekte Funktion der Verteilereinheiten während des Betriebes überwachen.

9. Verteilereinheit (101, 102) mit integriertem Guardian zur Erzwingung der fail-silent Eigenschaft im Zeitbereich von Knotenrechnern eines fehlertoleranten verteilten Computersystems, über welche eine Vielzahl von Knotenrechnern (111 ... 114) miteinander verbunden sind, jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit (211) mit zugehörigen Anschlüssen an die Kommunikationskanäle (201, 202) verfügt, und der Zugriff auf die Kommunikationskanäle entsprechend einem zyklischen Zeitscheibenverfahren erfolgt,

   dadurch gekennzeichnet, dass

   die zumindest eine Verteilereinheit (101, 102) dazu eingerichtet ist, aufgrund des ihr a priori bekannten regulären Sendeverhaltens der Knotenrechner zu erzwingen, dass ein Knotenrechner nur innerhalb seiner statisch zugewiesenen Zeitscheibe an die anderen Knotenrechner zu senden vermag.

10. Verteilereinheit (101, 102) nach Anspruch 9, eingerichtet zur Durchführung des Verfahrens nach einem der Ansprüche 2 bis 8.

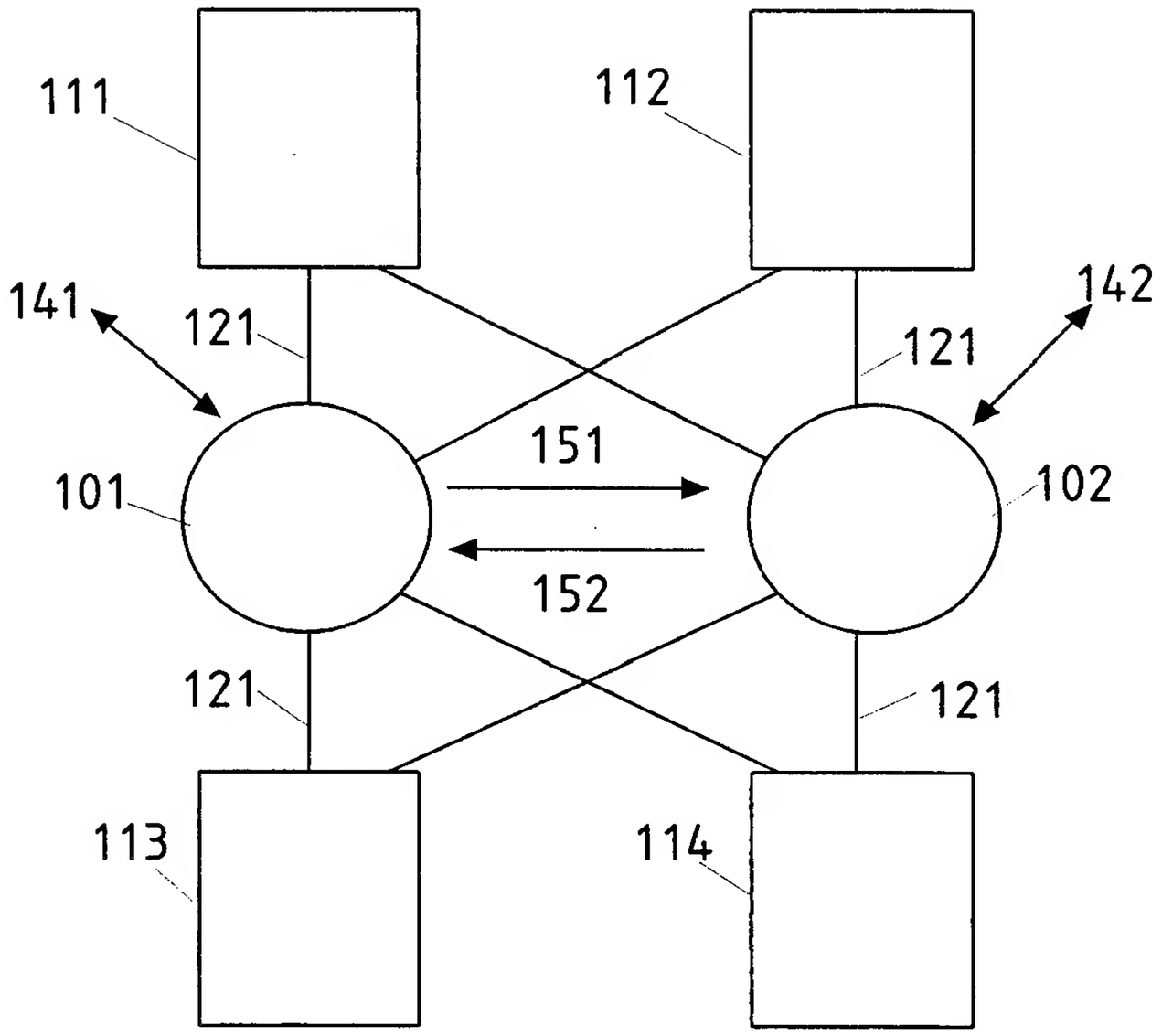

111
112
141
121
121
142
151
101
102
152
121
121
113
114

Fig. 1

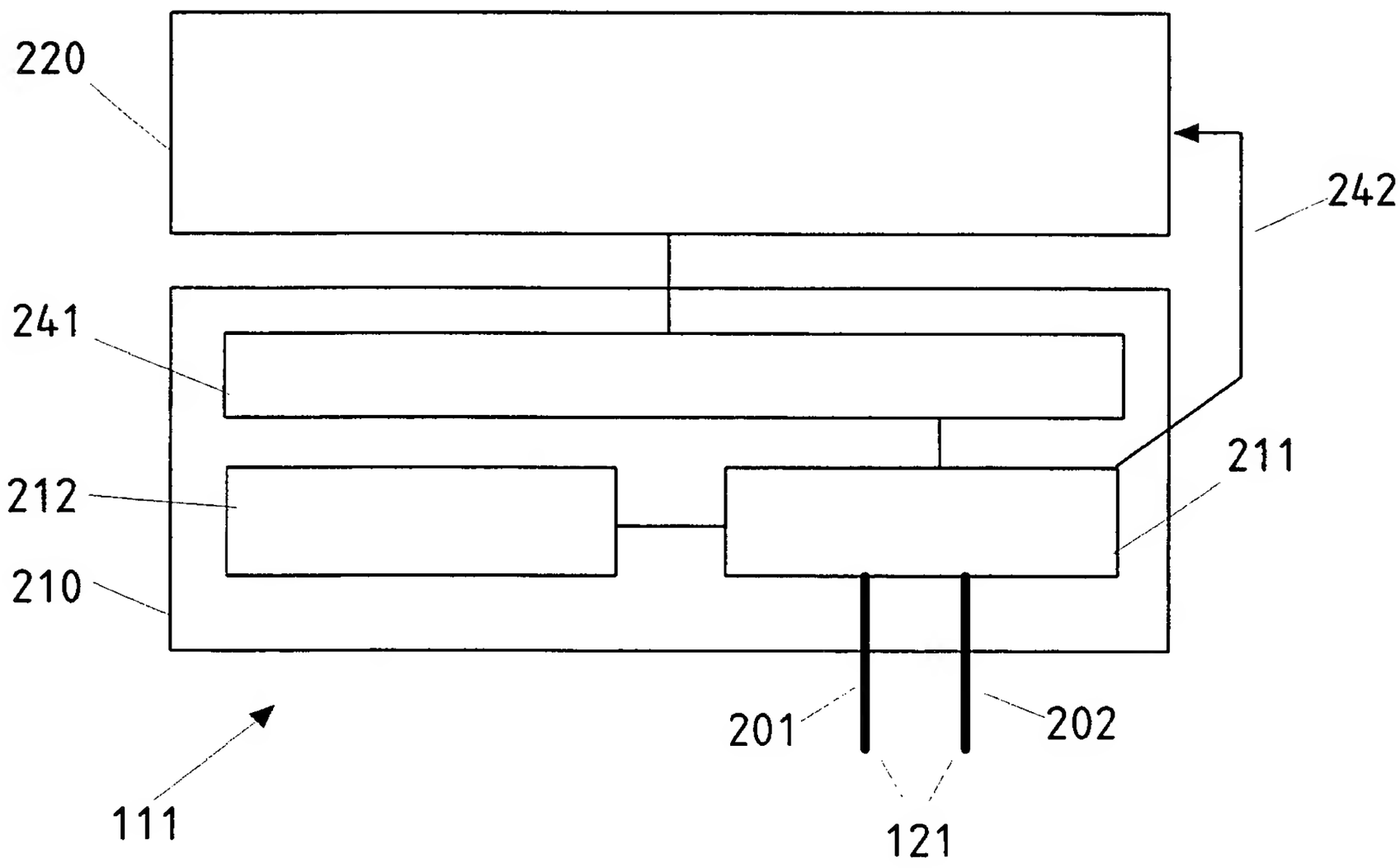

220
242
241
211
212
210
201
202
111
121

Fig. 2

2/2

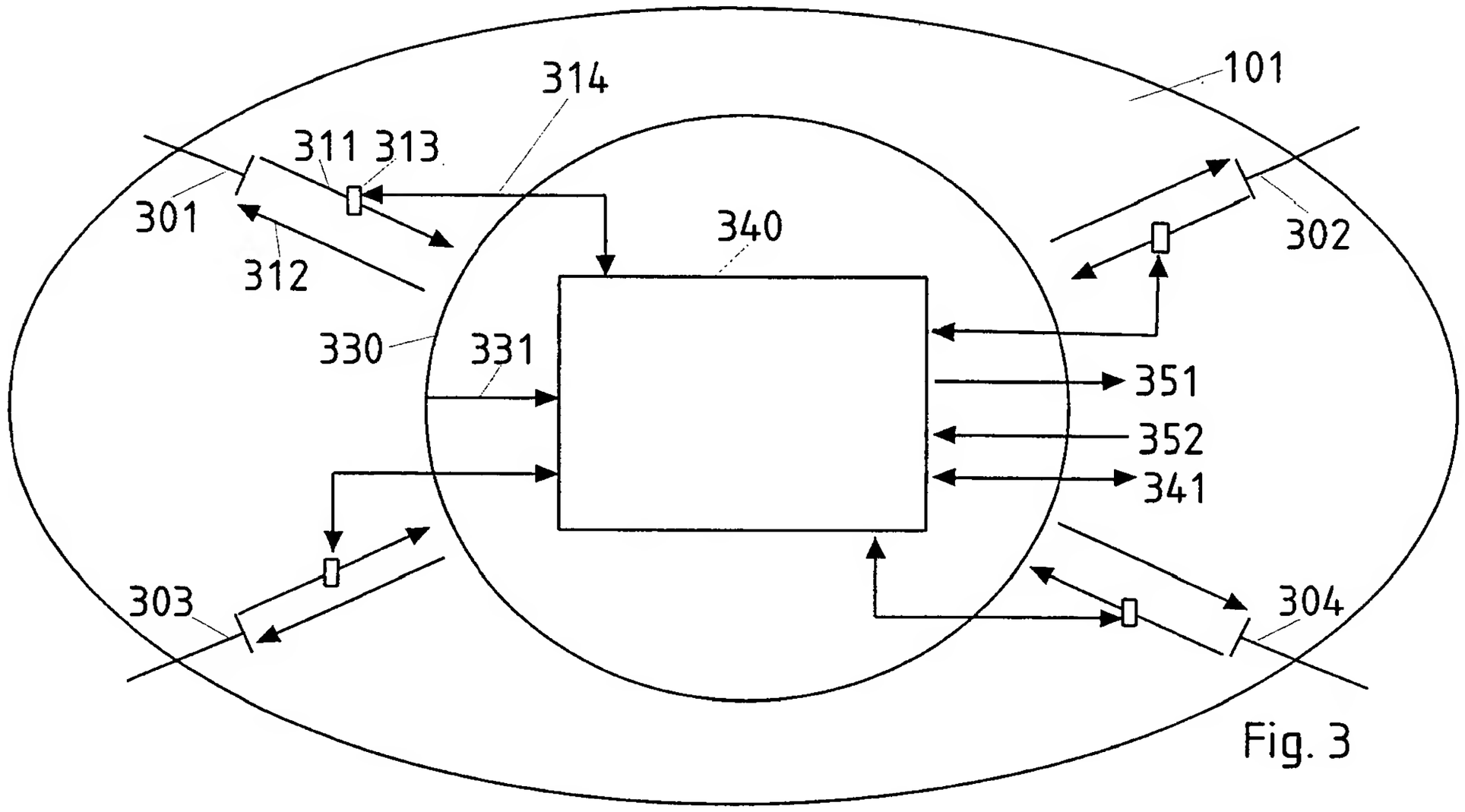


Fig. 3

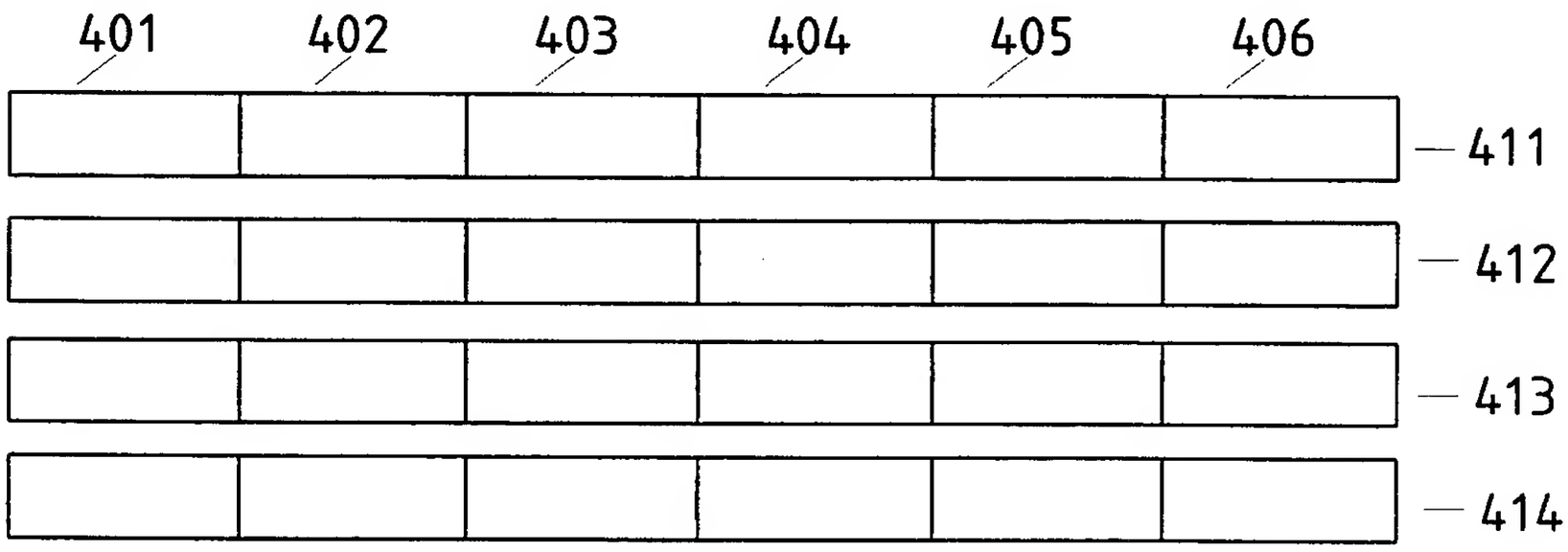


Fig. 4

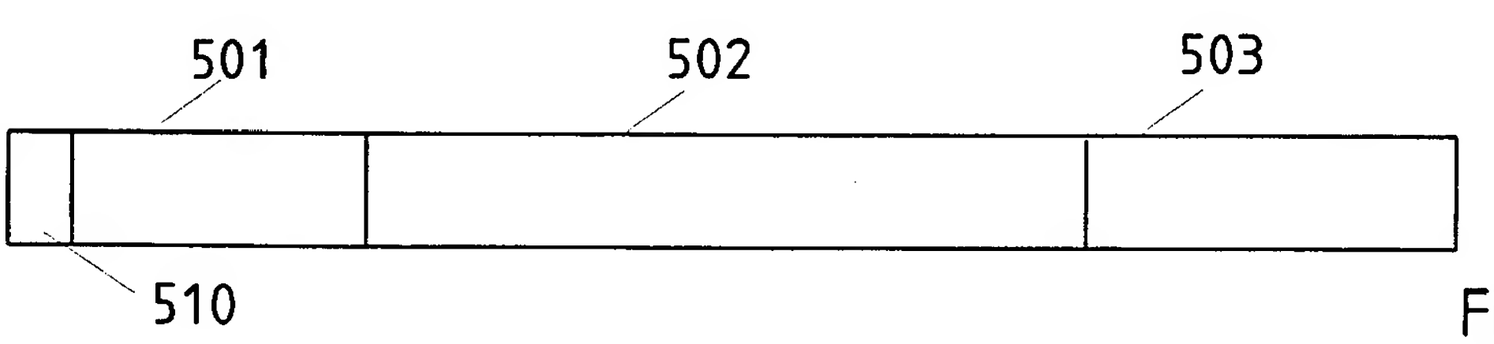


Fig. 5

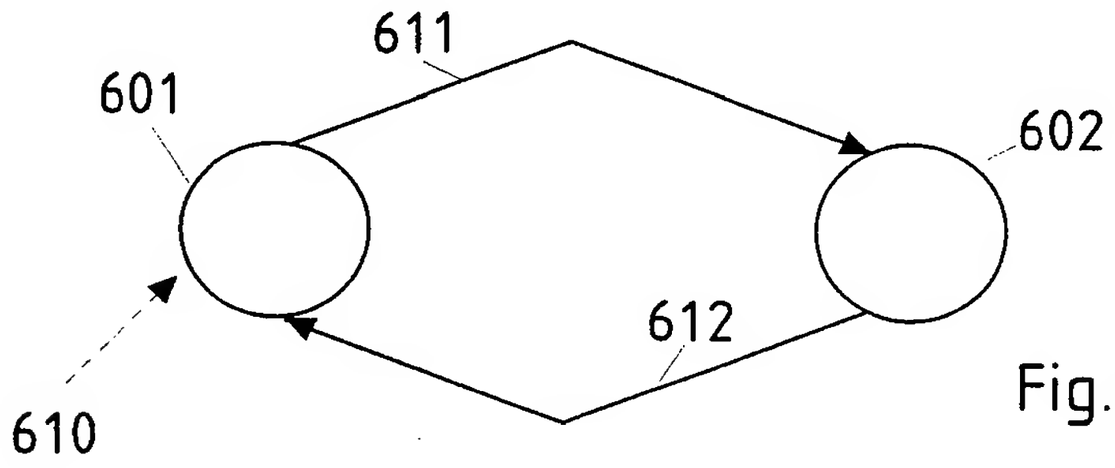


Fig. 6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/AT 00/00174

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TEMPLE C: "AVOIDING THE BABBLING-IDIOT FAILURE IN A TIME-TRIGGERED COMMUNICATION SYSTEM" ANNUAL INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING,US,LOS ALAMITOS, CA: IEEE COMPUTER SOC, 23 June 1998 (1998-06-23), pages 218-227, XP000804717 ISBN: 0-8186-8471-2 paragraphs '02.2!,'02.3!,'0003!,'03.6! --- -/--	1,2,5,7

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 January 2001	02/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Leuridan, K

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/AT 00/00174

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 484 275 A (KATZMAN ET AL) 20 November 1984 (1984-11-20) column 1, line 41 - line 54 column 4, line 35 - line 48 column 4, line 67 -column 5, line 7 column 7, line 50 - line 68 column 17, line 36 - line 46 column 20, line 40 -column 23, line 33 column 40, line 1 - line 8 figures 6,9	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/AT 00/00174

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4484275 A	20-11-1984	US 4228496 A	14-10-1980
		BE 892627 A	16-07-1982
		CA 1121481 A	06-04-1982
		CA 1176338 A	16-10-1984
		CA 1135809 A	16-11-1982
		CA 1147474 A	31-05-1983
		CA 1137582 A	14-12-1982
		CA 1147824 A	07-06-1983
		CA 1142619 A	08-03-1983
		CA 1136728 A	30-11-1982
		CA 1147417 A	31-05-1983
		CA 1185670 A	16-04-1985
		DE 2740056 A	16-03-1978
		FR 2473197 A	10-07-1981
		FR 2485227 A	24-12-1981
		FR 2485228 A	24-12-1981
		FR 2547082 A	07-12-1984
		GB 1588804 A	29-04-1981
		GB 1588805 A	29-04-1981
		GB 1588806 A	29-04-1981
		GB 1588807 A	29-04-1981
		GB 1588803 A	29-04-1981
		HK 62281 A	24-12-1981
		HK 62381 A	24-12-1981
		HK 62481 A	17-12-1981
		HK 62581 A	24-12-1981
		HK 62681 A	24-12-1981
		JP 1353183 C	11-12-1986
		JP 58050062 A	24-03-1983
		JP 61020017 B	20-05-1986
		JP 1257068 C	29-03-1985
		JP 53033027 A	28-03-1978
		JP 59025257 B	15-06-1984
		JP 61286962 A	17-12-1986
		JP 1408240 C	27-10-1987
		JP 60100252 A	04-06-1985
		JP 62018951 B	25-04-1987
		JP 1353197 C	11-12-1986
		JP 60100253 A	04-06-1985
		JP 61020018 B	20-05-1986
		JP 1353198 C	11-12-1986
		JP 60100254 A	04-06-1985
		JP 61020016 B	20-05-1986
		JP 1356211 C	24-12-1986
		JP 60100255 A	04-06-1985
		JP 61024740 B	12-06-1986
		JP 1359881 C	30-01-1987
		JP 60100256 A	04-06-1985
		JP 61029028 B	03-07-1986
		JP 1353199 C	11-12-1986

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT 00/00174

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F11/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, INSPEC, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	TEMPLE C: "AVOIDING THE BABBLING-IDIOT FAILURE IN A TIME-TRIGGERED COMMUNICATION SYSTEM" ANNUAL INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING,US,LOS ALAMITOS, CA: IEEE COMPUTER SOC, 23. Juni 1998 (1998-06-23), Seiten 218-227, XP000804717 ISBN: 0-8186-8471-2 Absätze '02.2!,'02.3!,'0003!,'03.6! --- -/--	1,2,5,7

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
26. Januar 2001	02/02/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Leuridan, K

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT 00/00174

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 4 484 275 A (KATZMAN ET AL) 20. November 1984 (1984-11-20) Spalte 1, Zeile 41 - Zeile 54 Spalte 4, Zeile 35 - Zeile 48 Spalte 4, Zeile 67 -Spalte 5, Zeile 7 Spalte 7, Zeile 50 - Zeile 68 Spalte 17, Zeile 36 - Zeile 46 Spalte 20, Zeile 40 -Spalte 23, Zeile 33 Spalte 40, Zeile 1 - Zeile 8 Abbildungen 6,9 -----	1-5

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/AT 00/00174

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 4484275 A	20-11-1984	US 4228496 A	14-10-1980
		BE 892627 A	16-07-1982
		CA 1121481 A	06-04-1982
		CA 1176338 A	16-10-1984
		CA 1135809 A	16-11-1982
		CA 1147474 A	31-05-1983
		CA 1137582 A	14-12-1982
		CA 1147824 A	07-06-1983
		CA 1142619 A	08-03-1983
		CA 1136728 A	30-11-1982
		CA 1147417 A	31-05-1983
		CA 1185670 A	16-04-1985
		DE 2740056 A	16-03-1978
		FR 2473197 A	10-07-1981
		FR 2485227 A	24-12-1981
		FR 2485228 A	24-12-1981
		FR 2547082 A	07-12-1984
		GB 1588804 A	29-04-1981
		GB 1588805 A	29-04-1981
		GB 1588806 A	29-04-1981
		GB 1588807 A	29-04-1981
		GB 1588803 A	29-04-1981
		HK 62281 A	24-12-1981
		HK 62381 A	24-12-1981
		HK 62481 A	17-12-1981
		HK 62581 A	24-12-1981
		HK 62681 A	24-12-1981
		JP 1353183 C	11-12-1986
		JP 58050062 A	24-03-1983
		JP 61020017 B	20-05-1986
		JP 1257068 C	29-03-1985
		JP 53033027 A	28-03-1978
		JP 59025257 B	15-06-1984
		JP 61286962 A	17-12-1986
		JP 1408240 C	27-10-1987
		JP 60100252 A	04-06-1985
		JP 62018951 B	25-04-1987
		JP 1353197 C	11-12-1986
		JP 60100253 A	04-06-1985
		JP 61020018 B	20-05-1986
		JP 1353198 C	11-12-1986
		JP 60100254 A	04-06-1985
		JP 61020016 B	20-05-1986
		JP 1356211 C	24-12-1986
		JP 60100255 A	04-06-1985
		JP 61024740 B	12-06-1986
		JP 1359881 C	30-01-1987
		JP 60100256 A	04-06-1985
		JP 61029028 B	03-07-1986
		JP 1353199 C	11-12-1986